



# SECS 1030

## labo Pi-Hole

**Noté 16 points – 10 % de la note finale**

Objectif du laboratoire : installez et utilisez un serveur DNS Sinkhole sur VirtualBox

Machine virtuelle : VM Ubuntu sur VirtualBox

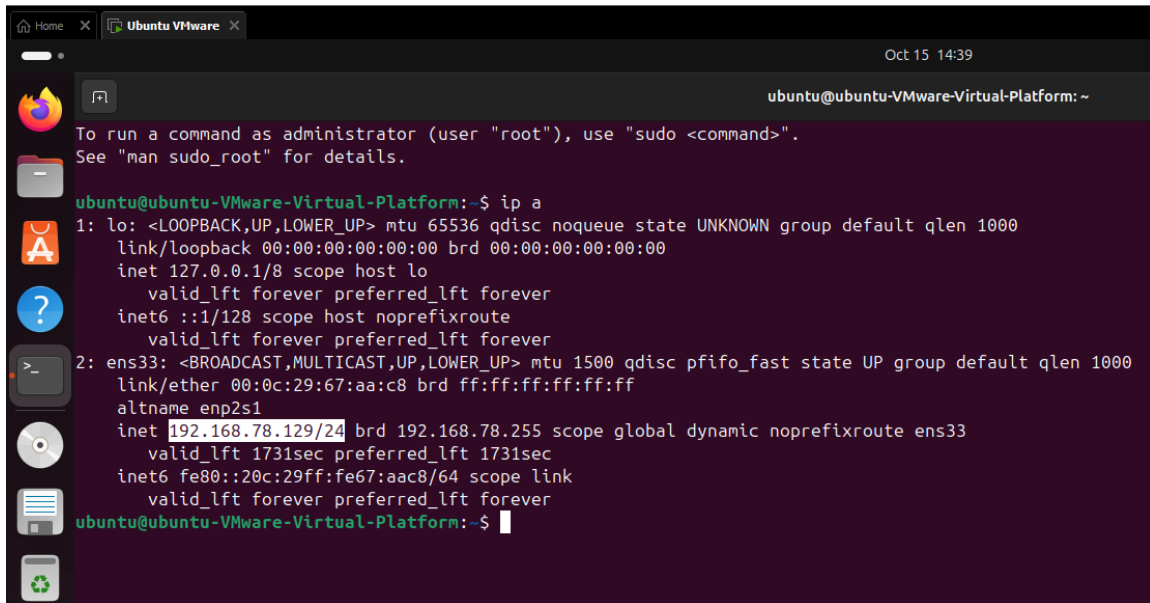
### Exercice 1 :

- 1) Question préliminaire : Qu'est-ce qu'un DNS Sinkhole?

Un mécanisme qui protège les utilisateurs en interceptant les requêtes DNS de domaine non voulu ou connu comme malveillant.

- 2) Téléchargez et installez la dernière version de Linux Ubuntu sur VirtualBox sur réseau NAT. Quelle est sa version ? Quelle est son adresse IP ?

## Ubuntu 24.04.1



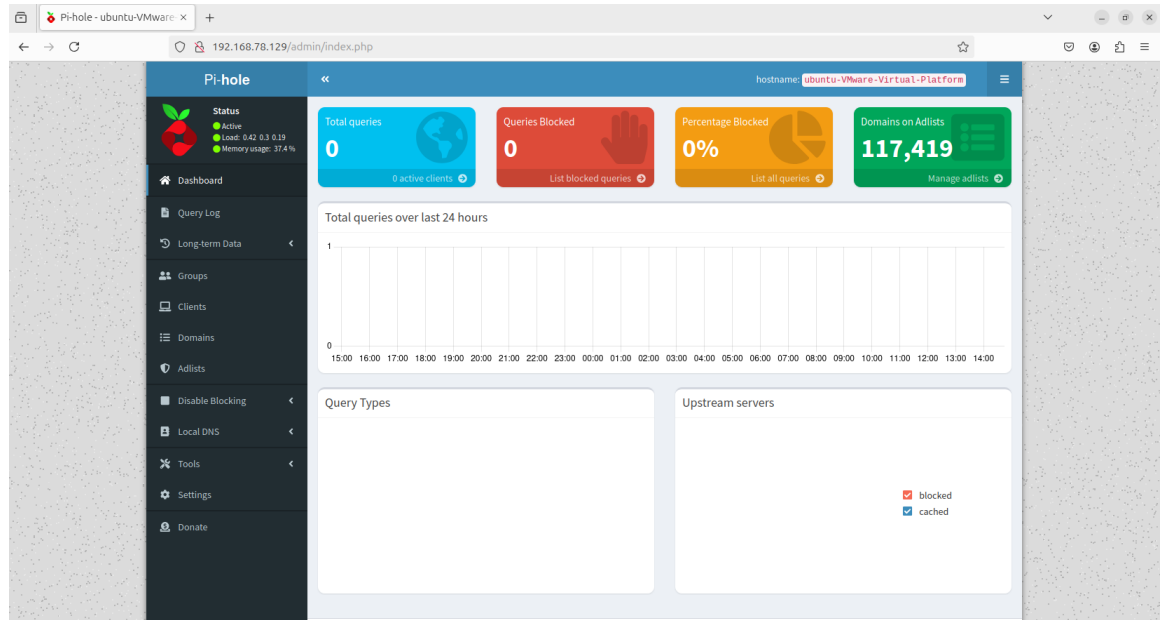
The screenshot shows a terminal window titled 'Ubuntu VMWare' with a dark background. The prompt is 'ubuntu@ubuntu-VMware-Virtual-Platform: ~'. The output of the 'ip a' command is displayed, showing details for the loopback interface 'lo' and the ethernet interface 'ens33'. The IP address for 'ens33' is 192.168.78.129/24.

```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:67:aa:c8 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.78.129/24 brd 192.168.78.255 scope global dynamic noprefixroute ens33
        valid_lft 1731sec preferred_lft 1731sec
    inet6 fe80::20c:29ff:fe67:aac8/64 scope link
        valid_lft forever preferred_lft forever
ubuntu@ubuntu-VMware-Virtual-Platform:~$
```

- 3) Télécharger et installez Pi-Hole sur la VM Ubuntu en suivant les instructions du site : <https://docs.pi-hole.net/main/basic-install/> . Faites la capture écran lorsque l'installation est complète :

## Exercice 2 : Configurer Pi-Hole

- 1) Ouvrez la page d'administration de Pi-Hole et faites une capture écran :



2) Que représente le nombre dans le carré vert en haut à droite « domains on adlists » ?

Liste de domaine et ad à bloquer

3) Dans Pi-Hole, quelle est la différence entre blacklist et whitelist ?

Blacklist : Domaine bloqué Whitelist : Domaine autorisé

4) Quelle est la différence entre un filtre de domaine et un filtre regex ?

Filtre de domain : blocage ou autorisation exact, Filtre regex : comprend tous les subdomain.

5) Créez un filtre permettant de bloquer l'accès au site example.com. Quel est ce filtre ?

Blacklist example.com

6) Démontrez que le filtre fonctionne en montrant les query logs (capture écran)

Pi-hole - ubuntu-VMware x Problem loading page x +  
 192.168.78.129/admin/queries.php?forwarddest=blocked

Pi-hole  
 Status  
 Active  
 Load: 1.53 1.02 0.62  
 Memory usage: 42.6%

Dashboard  
 Query Log  
 Long-term Data  
 Groups  
 Clients  
 Domains  
 Adlists  
 Disable Blocking  
 Local DNS  
 Tools  
 Settings  
 Donate

Recent Queries (showing queries blocked by Pi-hole)

Search: Type / Domain / Client  
 Previous 1 2 Next

Show 10 entries

Time	Type	Domain	Client	Status	Reply	Action
2024-10-22 12:02:04	A	example.com	pi.hole	Blocked (exact blacklist)	IP (0.0ms)	Whitelist
2024-10-22 12:02:02	A	pgl.example.com	pi.hole	Blocked (gravity)	IP (0.0ms)	Whitelist
2024-10-22 12:02:02	A	example.com	pi.hole	Blocked (exact blacklist)	IP (0.0ms)	Whitelist
2024-10-22 12:01:46	A	pgl.example.com	pi.hole	Blocked (gravity)	IP (0.1ms)	Whitelist
2024-10-22 12:01:46	HTTPS	example.com	pi.hole	Blocked (exact blacklist)	NODATA (0.0ms)	Whitelist
2024-10-22 12:01:46	A	example.com	pi.hole	Blocked (exact blacklist)	IP (0.0ms)	Whitelist
2024-10-22 12:01:44	A	incoming.telemetry.mozilla.org	pi.hole	Blocked (gravity)	IP (0.0ms)	Whitelist
2024-10-22 12:00:59	A	example.com	pi.hole	Blocked (exact blacklist)	IP (2.1ms)	Whitelist
2024-10-22 11:59:51	A	pgl.example.com	pi.hole	Blocked (gravity)	IP (0.1ms)	Whitelist
2024-10-22 11:59:51	A	example.com	pi.hole	Blocked (exact blacklist)	IP (0.0ms)	Whitelist

Showing 1 to 10 of 19 entries  
 Previous 1 2 Next

press Ctrl+G

## Exercice 3 : Questions

- Sous la VM Ubuntu, affichez le contenu du fichier `/etc/resolv.conf` (capture écran).  
 Expliquez la ligne nameserver ...  
 L'adresse ip du serveur (DNS)

```

ubuntu@ubuntu-VMware-Virtual-Platform:~$ cat /etc/resolv.conf
# This is /run/systemd/resolve/resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients directly to
# all known uplink DNS servers. This file lists all configured search domains.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 192.168.78.129
nameserver 192.168.78.2
search localdomain
ubuntu@ubuntu-VMware-Virtual-Platform:~$ Mikael Lacroix

```

2. Pi-hole utilise quel port ? (Utilisez nmap ou netstat) . Capture écran :  
53

```

ubuntu@ubuntu-VMware-Virtual-Platform:~$ nmap -sV 192.168.78.129 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-22 13:11 ADT
Nmap scan report for 192.168.78.129
Host is up (0.00011s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
53/tcp    open  domain  dnsmasq pi-hole-v2.90+1
80/tcp    open  http    lighttpd 1.4.74

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.40 seconds
ubuntu@ubuntu-VMware-Virtual-Platform:~$ Mikael Lacroix

```

3. Dans un terminal, lancez une résolution de nom de domaine (avec dig) sur le domaine example.com. Affichez le résultat :

Quel serveur donne la réponse ? Quelle est la réponse ? Expliquez.

192.168.78.129

La requête passe par pi-hole avant d'être bloquer donc c'est normal que l'on voie le serveur avec l'Adresse de pi-hole.

```
ubuntu@ubuntu-VMware-Virtual-Platform:~$ dig example.com

; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44962
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;example.com.                IN      A

;; ANSWER SECTION:
example.com.                2       IN      A      0.0.0.0

;; Query time: 0 msec
;; SERVER: 192.168.78.129#53(192.168.78.129) (UDP)
;; WHEN: Tue Oct 22 13:16:56 ADT 2024
;; MSG SIZE rcvd: 56

ubuntu@ubuntu-VMware-Virtual-Platform:~$ Mikael Lacroix
```

4. Dans un terminal, lancez une résolution de nom de domaine (avec dig) sur le domaine example.com en forçant l'utilisation du serveur DNS 8.8.8.8. Capture écran du résultat :

```

ubuntu@ubuntu-VMware-Virtual-Platform:~$ dig example.com @8.8.8.8

; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> example.com @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26180
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 512
;; QUESTION SECTION:
;example.com.                IN      A

;; ANSWER SECTION:
example.com.                2804    IN      A      93.184.215.14

;; Query time: 40 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Tue Oct 22 13:56:56 ADT 2024
;; MSG SIZE rcvd: 56

ubuntu@ubuntu-VMware-Virtual-Platform:~$

```

5.

Quelle est la réponse ? Interprétez ce résultat. Pouvez-vous en déduire la faille pour un DNS SinkHole ?

Le serveur a répondu (93.184.215.14)

DNS spoofing

6. Pouvez-vous proposer une solution pour la faille trouvée dans la question précédente ?

DNSSEC keys, clé privée et publique

7. Dans la configuration de Pi-Hole, partie DNS, quelle est la différence entre Quad9 filtered et Quad9 unfiltered ?

Quad9 filtered : Filtre les requêtes et le DNSSEC est activé, Quad9 unfiltered: laisse passer les requêtes et le DNSSEC n'est pas activé.

8. Comment Pi-hole peut améliorer la sécurité d'un réseau ? donner un exemple concret.

Bloque les requêtes DNS vers des domaines malveillants ou suspects. Prévention des attaques de phishing et des téléchargements de malwares.  
Empêche les activités de tracking